ABSTRACT

An improved computer network security system and method, and a personal identifier device used for controlling network access, to provide real time authentication of both a person's identity and presence at a computer workstation. A new user is registered to a portable personal digital identifier device and, within the portable personal digital identifier device, an input biometric of the user is received and a master template is derived therefrom and securely maintained in storage. A private key is also generated and securely maintained in the storage and a public key corresponding to the private key is generated and provided for external storage (in the network). A public key corresponding to a private key associated with a network security manager component is also stored in the device storage. When the personal digital identifier device is within an envelope area proximate the workstation a first signal is transmitted from a base unit associated with the workstation to the personal digital identifier device and the personal digital identifier device automatically transmits a response signal establishing communications between the base unit and the personal digital identifier device. The personal digital identifier device verifies the origin of a digitally signed challenge message from the network security manager component. A digitally and biometrically signed challenge response message is produced and transmitted by the personal digital identifier device in response to the verified challenge message. An image of the user may be displayed on the workstation screen when the user's personal digital identifier device is located within the envelope.